ABSTRACT

An electronic system and method for providing secure communications between devices. The secure communications are maintained through use of an integrity check value (ICV) that accompanies a message. The ICV is used to determine whether the contents of a message have been modified during transmission. An efficient technique for producing the ICV involves bitwise arithmetic operations and "exclusive OR" operations between data associated with the message (in its non-encrypted format) and coefficients of a matrix. The "coefficients" are selected bits from a pseudo-random data stream created by a cipher engine from keying material used in communications between the devices.